Социологические науки

УДК 004

Р.Х. Багдасарян

Е.А. Горбатко

Багдасарян Рафаэль Хачикович, кандидат технических наук, доцент кафедры библиотечно-библиографической деятельности и информационных технологий Краснодарского государственного института культуры (Краснодар, ул. им. 40-летия Победы, 33), e-mail: rafael_555@mail.ru

Горбатко Екатерина Андреевна, студентка 4 курса информационно-библиотечного факультета Краснодарского государственного института культуры (Краснодар, ул. им. 40-летия Победы, 33), e-mail: katya_gorbatko1441@icloud.com

АСПЕКТЫ УДАЛЕННОЙ РАБОТЫ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В УСЛОВИЯХ ЛОКДАУНА ОТ COVID-19

В данной статье исследуется механизм безопасности во время удаленной работы в условиях локдауна от COVID-19 при использовании современных информационных технологий. Авторами выявлены и проанализированы проблемы безопасности процесса удаленной работы. Также представлены рекомендации для эффективной защиты и снижения рисков информационной безопасности при использовании приложений и программ при дистанционной работе.

***Ключевые слова*:** информационная безопасность, информационные технологии, пандемия COVID-19, кибербезопасность, дистанционная работа, телеработа.

R.Kh. Bagdasaryan

E.A. Gorbatko

Baghdasaryan Rafael Khachikovich, candidate of technical sciences, associate professor of department of library and bibliographic activity and information technologies of the Krasnodar state institute of culture (33, im. 40-letiya Pobedy st., Krasnodar), e-mail: rafael_555@mail.ru.

Gorbatko Ekaterina Andreevna, 4th course student of information and library faculty of the Krasnodar state institute of culture (33, im. 40-letiya Pobedy st., Krasnodar), e-mail: katya_gorbatko1441@icloud.com

ASPECTS OF REMOTE WORK USING INFORMATION TECHNOLOGY IN A PANDEMIC COVID-19

This scientific article examines the mechanism of security during remote work in the conditions of the COVID-19 pandemic, using information technology. The author identified and analyzed the security problems of the remote work process. Recommendations for effective protection and reduction of information security risks when using applications and programs for remote work are presented. Thus, with the right selection of protection tools, and the regulatory and methodological framework for ensuring information security, this goal and objectives can be solved.

Key words: information security, information technologies, COVID-19 pandemic, cybersecurity, remote work, teleworking.

Беспрецедентный по своему масштабу, скорости и глубине кризис, вызванный пандемией и многочисленными локдаунами городов от COVID-19, привел к разбалансировке всего и дестабилизации на национальных рынках труда [2].

Ежедневно по всему миру пандемия создает напряженную обстановку в сфере здравоохранения, что сильно влияет на экономику различных стран и регионов. Согласно данным международной организации труда (МОТ), COVID-19 привел к самому серьезному кризису в сфере труда со времен Великой депрессии 1930-х годов [3]. Данные изменения непосредственно затронули также всю сферу труда. Так, в 2020 году было потеряно в общей сложности 8,8% рабочего времени, что эквивалентно и равносильно годовой продолжительности часов работы 255 млн работников, занятых на условиях полного рабочего дня [4]. В целях предотвращения распространения пандемии COVID-19 были приняты различные меры общественного здравоохранения и контроля, согласно рекомендациям Всемирной организации здравоохранения (ВОЗ), которые менялись каждый раз при вновь возникавших эпидемиологических ситуациях. Для того чтобы сдержать распространение вируса и его разного рода штаммов, одними из главных мер, предпринятых властями стран, являются физическое дистанцирование и сокращение физических контактов. В связи с этим на сегодняшний день проблемой больше миллиона компаний стало дистанционное управление рабочей силы при помощи информационных технологий в условиях пандемии COVID-19.

Удаленный режим работы (УРР) – это способ организации труда, при котором работник выполняет важнейшие функции, связанные со своей работой, с помощью информационно-коммуникационных технологий (ИКТ), при этом находясь дома [5]. Основой быстрого перехода организаций к удаленной работе во время пандемии COVID-19 стали цифровой прорыв и массовое оперативное информационное окультуривание работников, а также быстрое замещение поставщиками различных технологий на

информационные продукты и услуги, которые в том числе предоставляют программные решения, устраняющие сложность и дающие гарантию эффективного и безопасного управления информационными технологиями. Аналогичным образом организации во всех секторах внедряют политику удаленной работы для своих сотрудников в соответствии с этой тенденцией [6]. На сегодняшний день известно много отечественных решений в области информационной безопасности и международных рекомендаций по организации безопасного удаленного доступа.

В целях предупреждения риска взлома систем и несанкционированного доступа к данным, а именно – для устранения рисков кибербезопасности, которые приводят к потере данных, порче репутации и технологического спада, организациям необходимо предпринимать следующие действия:

– в связи с неэффективными системами управления паролями и для устранения рисков кибербезопасности удаленных работников необходимо предпринять усиленные меры по улучшению управления паролями, а именно – необходимо объединить единый вход с таким компонентом управления доступом, как многофакторная аутентификация;

– большинство компаний переходят к удаленным сотрудникам, тем самым используя в работе виртуальные рабочие столы, где основной причиной перехода является предупреждение потери данных. Вся информация на рабочий стол передается из защищенного частного центра обработки данных или из общедоступного облака, благодаря которым секретные бизнес-данные не оказываются на удаленных рабочих столах, где они могут явиться случайными или специальными утечками;

– необходимо обучать и предоставлять необходимые материалы удаленным работникам по безопасности work from home – «работы из дома», а именно: как обрабатывать пароли, как защитить корпоративное оборудование, использовать авторизованные приложения для совместной работы, каким образом хранить конфиденциальные данные, как предотвратить риски теневой Information technology – IT (цифровые

инструменты, которые работники применяют без разрешения руководства компании) и безопасной проверки личности людей, с которыми работают удаленные работники.

За последние несколько лет наблюдается тенденция увеличения количества инцидентов, связанных с кибероружием и кибершпионажем. Данные обстоятельства находят проявление в регулярно обнаруживаемых программах, относящихся к кибероружию, – *Stuxnet, RedOctober, Winnti, IceFog* и др. Однако в настоящее время нет достоверных фактов, подтверждающих проведение атак на Россию со стороны других государств [1]. Во время пандемии COVID-19 множество компаний перевели своих работников в режим онлайн-работы. Весь мир информационных технологий столкнулся с информационной безопасностью. В России информационные технологии не являются совершенными, имеют множество недостатков, а ситуация с отдаленными районами огромного федеративного государства страны до конца не изучена, но данные проблемы еще не привели к национальному краху в Рунет (сеть интернет в России).

Необходимы дальнейшие улучшения нормативно-методической базы для совершенствования в полном объеме защищенного удаленного доступа, усовершенствования национальных высокоустойчивых архитектур, а также следует уделить большее внимание на развитие регионов Российской Федерации со слабым интернетом для применения в конечном итоге информационных технологий нового поколения. Таким образом, при правильном подборе инструментов защиты нормативно-методической базы обеспечения информационной безопасности данная цель и задачи могут быть решены.

Список используемой литературы:

1. *Навальный, С. В.* Информационная безопасность в России: пути обеспечения / С.В Навальный // Правовая политика и правовая жизнь. – 2015. – № 3. – С. 33–38.

2. *Подвойский, Г. Л.* Сфера труда в условиях пандемии COVID-19: анализ, оценки и рекомендации МОТ / Г.Л. Подвойский // Мир новой экономики. – 2021. – № 15(1). – С. 28–39.

3. Вестник МОТ: COVID-19 и сфера труда. Седьмой выпуск. Обновленные оценки и анализ // International Labour Organization (ILO): [сайт]. – 2021. URL: https://www.ilo.org/wcmsp5/groups/public/---europe/---ro-geneva/---sro-moscow/documents/briefingnote/wcms_767671.pdf (дата обращения: 21.10.2021).

4. Удаленный режим работы в условиях пандемии COVID-19: руководство для работодателей // International Labour Organization (ILO): [сайт]. – 2020. URL: https://www.ilo.org/wcmsp5/groups/public/---ed_dialogue/---act_emp/documents/publication/wcms_749872.pdf) (дата обращения: 21.10.2021).

5. *Emmitt, J.* Top 10 Cybersecurity Threats in 2020 // Kaseya: [website]. – 2020. URL: https://www.kaseya.com/blog/2020/04/15/top-10-cybersecurity-threats-in-2020/ (date access: 20.10.2021).

6. *Souppaya, M.* Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security / M. Souppaya, K. Scarfone // National Institute of Standards and Technology. – 2016. – № 2. URL: http://dx.doi.org/10.6028/NIST.SP.800-46r2 (date access: 20.10.2021).